ФСТЭК РОССИИ

УПРАВЛЕНИЕ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И
ЭКСПОРТНОМУ КОНТРОЛЮ
ПО СЕВЕРО-ЗАПАДНОМУ
ФЕДЕРАЛЬНОМУ ОКРУГУ
(Управление ФСТЭК России по
Северо-Западному федеральному округу)

Исаакиевская пл., д. 11, Санкт-Петербург, 190000
Тел./факс: 8 (812) 312-55-29
E-mail: szfo@fstec.ru

«30» 04 2020 г. № 7/514

На № _____

ОТЗЫВ

на автореферат диссертации Ушакова Игоря Александровича «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

В рамках достижения национальных целей развития Российской Федерации на период до 2024 г. реализуются проекты, направленные на цифровую трансформацию экономики и социальной сферы государства.

Их осуществление объективно приведет к расширению типов цифровых данных, разнообразию их источников, к увеличению объема информации, обрабатываемой в информационных системах органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций и, как следствие, к разнообразию информационных угроз.

В настоящее время в банке данных угроз безопасности информации ФСТЭК России, поддерживаемом в актуальном состоянии, содержится более 25 тыс. записей об уязвимостях программного обеспечения и более 200 записей об угрозах безопасности информации, наиболее характерных для государственных информационных систем, информационных систем персональных данных и автоматизированных систем управления технологическими процессами на критически важных объектах.

При этом статистические данные по анализу защищенности информационных систем свидетельствуют о том, что каждая третья крупная российская компания и каждая четвертая корпорация столкнулись с утечкой

14298

ООО «Типография «Евроколия-2 СПб». СПб. 2019 г. Зак. № 190094. Тир. 4 000 экз.

данных, при этом более 50% руководителей организаций считают, что наибольшую опасность для безопасности информации составляют сами сотрудники, в их числе имеющие доступ к инсайдерской информации лиц, перечисленных в статье 4 Федерального закона от 27.07.2010 № 224-ФЗ (ред. от 01.04.2020).

В диссертации соискатель рассматривает актуальную задачу информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.

Разработанный лично автором комплекс взаимосвязанных моделей, алгоритмов и методики, исходя из текста автореферата, позволяет:

а) выявить и идентифицировать инсайдерские угрозы нарушения информационной безопасности защищаемых объектов, реализуемые в форме инсайдерских атак;

б) оптимизировать процесс обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием внутренних угроз нарушения его информационной безопасности.

Как следует из автореферата, новизна предложенного научно-методического аппарата заключается в возможности реализации системы мероприятий по защите от деструктивного информационного воздействия с учетом предыстории протекания процесса инсайдерской деятельности в информационных системах любого вида и области применения.

В целом автореферат дает достаточно полное и всестороннее представление о работе и соответствует требованиям ВАК.

В качестве недостатков представленного автореферата диссертационной работы следует отметить следующее:

1. Представленный текст автореферата не дает полного представления об архитектуре предлагаемой автором системы обнаружения инсайдеров в компьютерных сетях, что позволяет лишь на концептуальном уровне иметь суждения об организации системы, а также принципах ее проектирования и эволюции.

2. Из текста автореферата (с.13) неясно какие существенные признаки использованы автором при определении понятия "атака инсайдеров" и его соотношение с другими понятиями специфической предметной области, например, "компьютерная атака" или "компьютерный инцидент".

Отмеченные недостатки носят уточняющий характер и не ставят под сомнение результаты работы.

Полученные автором результаты имеют научную ценность и практическую значимость.

Результаты работы апробированы на ряде международных конференций, имеются 9 публикаций в рецензируемых журналах из перечня ВАК («Вопросы кибербезопасности», «Защита информации. Инсайд», «Труды СПИИРАН», «Труды учебных заведений связи»).

В целом представленный автореферат позволяет сделать вывод о том, что диссертация является законченной научно-квалификационной работой, в которой изложено научно обоснованное техническое решение, имеющее существенное значение для развития страны.

Работа выполнена самостоятельно, на высоком научном уровне и соответствует классификационным признакам, определяющим характер результатов кандидатской диссертационной работы.

Полученные автором результаты достоверны, выводы и заключения обоснованы.

Диссертационная работа отвечает требованиям п. 9-14 Положения о присуждении учёных степеней, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 года, предъявляемым к кандидатским диссертациям, а ее автор, Ушаков Игорь Александрович, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Отзыв составил
Заместитель руководителя Управления ФСТЭК России
по Северо-Западному федеральному округу
кандидат военных наук, доцент

Шакин Дмитрий Николаевич

30.04.2020

11, г. Санкт-Петербург, 190000
(812) 571-16-77
@fstec.ru